UNITED STATES DISTRICT COURT FOR THE
SOUTHERN DISTRICT OF FLORIDA
FORT LAUDERDALE DIVISION

**Case No.: 25-cv-60803-WPD**

K.MIZRA LLC,

Plaintiff,

v.

CITRIX SYSTEMS, INC. and CLOUD SOFTWARE GROUP, INC.,

Defendants.
_______________________________________/

# DEFENDANTS' MOTION TO DISMISS K.MIZRA LLC'S COMPLAINT

## TABLE OF CONTENTS

# TABLE OF AUTHORITIES

Page(s)

## Cases

**Statutes**

**Other Authorities**

Pursuant to Rule 12(b)(6), Citrix Systems, Inc. and Cloud Software Group, Inc. ("Defendants") respectfully request that the Court dismiss K.Mizra LLC's ("K.Mizra") Complaint with prejudice because the asserted claims of U.S. Patent No. 8,234,705 ("the '705 patent") are not patent-eligible under 35 U.S.C. § 101.

## I. INTRODUCTION

There are three fundamental problems with the patent claims K.Mizra asserts against Defendants. First, the claims are directed to the abstract idea of protecting a network from an infected host through contagion isolation and inoculation, amounting to the well-known human practice of quarantine. Second, the patent itself explains that it did not invent the hardware and software components recited in the claims and that the components are neither novel nor used in a novel manner. Third, the ordered combination of claim limitations mirrors well-understood practice, adding nothing inventive. For each of these reasons, none of the asserted claims is eligible for patent protection.

The asserted patent claims fail the two-step test set out in *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208 (2014), and are therefore directed to ineligible subject matter. In *Alice*, the Supreme Court explained that a claim falls outside the scope of § 101 if: (1) it is directed to a patent-ineligible concept such as an abstract idea, and (2) it lacks an "inventive concept" sufficient to ensure that the claim amounts to significantly more than a claim upon the abstract idea itself. Here, each asserted claim is directed to the abstract idea of protecting a network from an infected host through contagion isolation and inoculation, and none of the claims, whether the limitations are considered individually or as an ordered combination, contains any inventive concept.

Courts have found similar claims to be directed to patent-ineligible abstract ideas. *See, e.g., Digital Media Techs., Inc. v. Hulu, LLC*, 2017 WL 4750705, at *7 (N.D. Fla. July 3, 2017); *Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App'x 1014, 1019 (Fed. Cir. 2017); *Ericsson Inc. v. TCL Commc'n Tech. Holdings Ltd.*, 955 F.3d 1317, 1331 (Fed. Cir. 2020). District courts have accordingly granted motions to dismiss with prejudice, and the Federal Circuit has repeatedly affirmed these dismissals. The Court should reach the same result here.

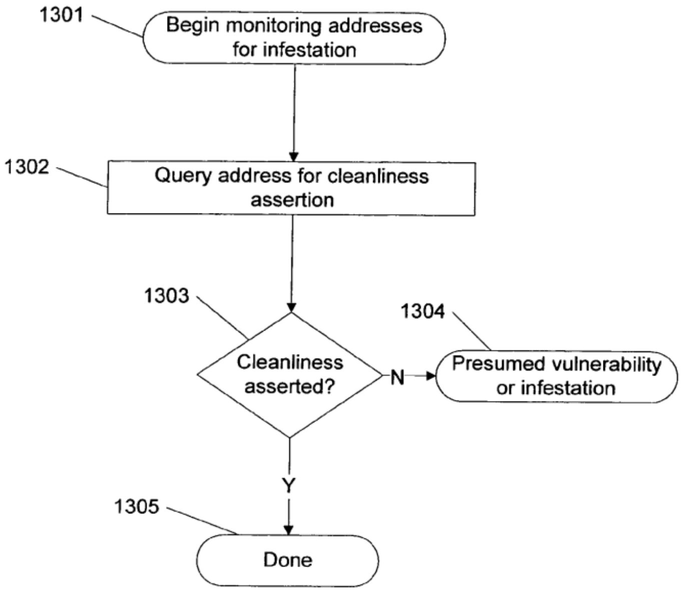
## II. FACTUAL BACKGROUND

### A. Overview of the '705 Patent

The '705 patent, which issued on July 31, 2012, is titled "Contagion Isolation and Inoculation." Dkt. 1, Ex. 4. K.Mizra alleges that the named inventors of the '705 patent decided to create a business "developing intellectual property related to various computer technologies" by "drafting patent applications to capture and protect" "inventions that they knew were needed (or soon would be needed) in the computer networking industry." Dkt. 1 ¶ 23. K.Mizra alleges that the '705 patent claims priority to U.S. Provisional Application No. 60/613,909, filed on September 27, 2004, a decade before the Supreme Court's *Alice* decision. Dkt. 1 ¶ 19. That provisional application concerned securing a computer network against threats when hosts are connected to the network, and quarantining and remedying those threats. Dkt. 1 ¶ 23.

The '705 patent explains that hosts, such as laptop computers, pose a threat to protected networks. Dkt. 1 ¶ 25. These hosts may reconnect to a protected network after being connected to systems that are not part of the protected network. '705 patent at 1:14-20. Upon reconnecting to the protected network, the host may infect or harm the protected network before measures can be taken to detect and prevent the spread of such harm. '705 patent at 1:20-38. The inventors believed existing "network security appliance[s] or hardware can be adept at keeping out unwanted external intrusions from the network." Dkt. 1 ¶ 24. Instead, they focused on "the end-user computers [hosts] that roam throughout various public and private network domains." *Id.*

The '705 patent includes an illustration of "a method for monitoring one or more computers for infestation according to some embodiments." '705 patent at 13:54-56.


1301
Begin monitoring addresses for infestation
1302
Query address for cleanliness assertion
1303
Cleanliness asserted?
N
1304
Presumed vulnerability or infestation
Y
1305
Done

'705 patent, Fig. 13. The '705 patent describes that monitoring begins at step **1301** "by retrieving a list of one or more addresses of computers, such as addresses of participating subscribers," which are possible hosts. *Id.* at 13:57-59. Next, a "computer associated with an address identified in a list is queried for a cleanliness assertion (**1302**), for example by contacting a trusted computing base within a computer, and requesting an authenticated infestation scan by trusted software." *Id.* at 13:64-14:1. "If a computer asserts it is clean (**1303**) then monitoring is complete (**1305**) in this example. If a cleanliness assertion is not provided (**1303**) then an infestation or vulnerability is presumed (**1304**) in this example." *Id.* at 14-:23-26.

### B. The State of the Art at the Priority Date of the '705 Patent

The '705 patent did not invent "contacting a trusted computing base within a computer." Instead, the patent discloses examples that had already been invented, including "the Paladium security initiative under development by Microsoft and supported by Intel and American Micro Devices," and the trusted computing base "described in various TCG specifications, such as the TCG Architecture Overview, published by the Trusted Computing Group." *Id.* at 14:1-7. The '705 patent also describes behaviors of these trusted computing bases: "for example execute antivirus scans of the remainder of the computer," or "digitally sign assertions about the cleanliness (e.g. infestation status) and/or state of their computers." *Id.* at 14:7-12. These existing hardware components were already known, their purpose was well understood, and the claim language referring to "attestations" of cleanliness that are "digitally signed" mirrors the terminology used in the prior art cited by the '705 patent.

The claims of the '705 patent describe a well-known concept implemented on a computer. K.Mizra alleges that the claims are directed to a process with four steps:

> (1) determining whether the host computer is required to be quarantined, (2) isolating and inoculating the contagions (including directing the host to software programs and/or code designed to identify undesirable and/or unauthorized states) by quarantining the host, (3) limiting access to the network by the host computer so that the unsafe condition thereof can be remedied, and (4) allowing for remediation of an unsafe or infected host computer.

Dkt. 1 ¶ 34. Though the patent's title, "Contagion Isolation and Inoculation," calls to mind the global pandemic experienced in recent years, the human practice of quarantine is ancient. An example of this practice described over two decades ago is found in the 2004 Florida Statute for school-entry health examinations, immunization against communicable diseases, and exemptions thereto. § 1003.22, Fla. Stat. (2004).

In 2004, when the provisional application preceding the '705 patent was filed, the state of Florida required immunizations for "communicable diseases as determined by rules of the Department of Health," including polio, diphtheria, and mumps. *See* Ex. 1 (§ 1003.22, Fla. Stat.

(2004)). In relevant part, the law required that,

> prior to admittance to or attendance in a public or private school, grades kindergarten through 12, or any other initial entrance into a Florida public or private school, each child present or have on file with the school a certification of immunization for the prevention of those communicable diseases for which immunization is required.

As shown in the table below, the Florida legislature set forth requirements that school boards require health examinations for entry and refuse to admit or temporarily exclude children without certification of immunization. To effectuate its goals, it further required each local school health services plan to assist students in obtaining health examinations, and required immunizations be made available at no cost. Moreover, it mandated that the "transfer of such immunization certification by Florida public schools shall be accomplished using the Florida Automated System for Transferring Education Records and shall be deemed to meet the requirements of this section." A comparison between K.Mizra's description of the asserted patent claims and the Florida 2004 immunization statute is revealing.

| **K.Mizra (Dkt. 1 ¶ 34): "The Asserted Claims are thus directed to a machine-implemented process for:** | **Section 1003.22, Florida Statutes (2004):** |
|---|---|
| (1) determining whether the host computer is required to be quarantined, | "(1) Each district school board and the governing authority of each private school shall require that each child who is entitled to admittance to kindergarten, or is entitled to any other initial entrance into a public or private school in this state, present a certification of a school-entry health examination performed within 1 year prior to enrollment in school." |
| (2) isolating and inoculating the contagions (including directing the host to software programs and/or code designed to identify undesirable and/or unauthorized states) by quarantining the host, | "Any district school board that establishes such a policy shall include provisions in its local school health services plan to assist students in obtaining the health examinations."<br>"(4) Each district school board and the governing authority of each private school shall establish and enforce as policy that, prior to admittance to or attendance in a public or private school, grades kindergarten through 12, or any other initial entrance into a Florida public or private school, each child present or have on file with the school a certification of immunization for the prevention of those communicable diseases for which immunization is required by the Department of Health . . . ." |

| | |
|---|---|
| (3) limiting access to the network by the host computer so that the unsafe condition thereof can be remedied, and | "(10) Each district school board and the governing authority of each private school shall: (a) Refuse admittance to any child otherwise entitled to admittance to kindergarten, or any other initial entrance into a Florida public or private school, who is not in compliance with the provisions of subsection (4) [requiring certification of immunization]. (b) Temporarily exclude from attendance any student who is not in compliance with the provisions of subsection (4) [requiring certification of immunization]." |
| (4) allowing for remediation of an unsafe or infected host computer." | "Immunizations shall be required for poliomyelitis, diphtheria, rubeola, rubella, pertussis, mumps, tetanus, and other communicable diseases as determined by rules of the Department of Health. The manner and frequency of administration of the immunization or testing shall conform to recognized standards of medical practice. The Department of Health shall supervise and secure the enforcement of the required immunization. Immunizations required by this section shall be available at no cost from the county health departments." |

As shown above, the claims of the '705 patent are directed to the well-known human practice of treating potentially infected hosts through isolation, inoculation, and remediation. The ordered steps of this age-old practice, as enacted in the laws of Florida at the time of the patent's priority date, are analogous to the steps of the asserted claims—steps directed to the abstract idea of protecting a network from an infected host through contagion isolation and inoculation.

### C. Overview of the Asserted Claims

K.Mizra alleges infringement of "one or more claims of the '705 patent." Dkt. 1 ¶ 44. The '705 patent has 19 claims, of which three—1, 12, and 19—are independent claims. While K.Mizra's allegations mention claim 19 (*id.* ¶¶ 45-55), the Complaint does not specifically articulate infringement allegations regarding the other 18 claims of the '705 patent. However, those claims do not significantly differ from claim 19, and there are no material differences for purposes of determining their lack of subject-matter eligibility. Claim 19 is reproduced below:

> [preamble] A computer program product for protecting a network, the computer program product being embodied in a non-transitory computer readable medium and comprising computer instructions for:
>
> [A] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,
>
> [B] wherein detecting the insecure condition includes:

> > [B1] contacting a trusted computing base associated with a trusted platform module within the first host,
> >
> > [B2] receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness,
>
> [C] wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;
>
> [D] when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,
>
> [E] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes
>
> > [E1] receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request,
> >
> > [E2] and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and
>
> [F] permitting the first host to communicate with the remediation host.

Dkt. 1 ¶ 44; *see also* ’705 patent at 22:14-49. As K.Mizra acknowledges, the “other independent claims of the ’705 Patent—Claims 1 and 12—are directed to a method and system, respectively, for protecting a secure network and having many of the same limitations included in claim 19.” *See* Ex. 2 (*K.Mizra LLC v. Hewlett Packard Enter. Co. and Aruba Networks*, No.: 2:21-cv-00305-JRG, Doc. 202 (E.D. Tex. Mar. 7, 2024)) at 3.

The dependent claims of the ’705 patent are also not materially different for purposes of determining their lack of subject-matter eligibility. For example, claim 9 recites, “A method as recited in claim 1, wherein the software component on the first host is an operating system.” Dependent claims 2, 4, 7, 9, 10, and 11, which each depend from claim 1, are mirrored in dependent claims 13-18, which each depend from claim 12. So, for example, much like claim 9, claim 16 recites, “A system as recited in claim 12, wherein the software component on the first host is an operating system.” The other dependent claims likewise designate conditions about what constitutes terms already included in the independent claims. Claims 2, 3, 4, 13, and 14 further relate to detection of an "insecure condition," and claims 10, 11, 17, and 18 similarly connect the claimed determinations to whether an update or patch is sufficiently recent. Claims 5, 6, 7, and 15 relate to what constitutes permitting and preventing communication. Finally, claim 8 states simply, "A method as recited in claim 1, performed at an Internet service provider."

To summarize, independent claims 1, 12, and 19 are substantially similar. The dependent claims do not alter or differ from the concept recited in the independent claims—instead, they each refer to claim terms in the independent claims, and designate conditions about those terms. The claims therefore do not meaningfully differ for analyzing patent eligibility, because they are all linked to the same abstract idea of protecting a network from an infected host through contagion isolation and inoculation and have no material differences for the § 101 analysis.

### D. Prosecution History of the '705 Patent

The application that issued as the '705 patent was filed on Sep. 27, 2005. During prosecution, the examiner issued office actions, each of which rejected the claims as unpatentable over prior art, on November 14, 2008, July 9, 2009, July 20, 2010, and October 12, 2011. *See* Ex. 3 (Relevant Prosecution History Excerpts).[1] Patent eligibility based on subject matter under § 101 was not raised during prosecution. The entire prosecution of the '705 patent took place prior to the Supreme Court's *Alice* decision in 2014 which clarified and established the applicable law of patent eligibility based on subject matter under § 101. *Alice*, 573 U.S. at 208.

K.Mizra alleges "[a]ll claims of the ['705 patent] are also presumed to be valid and enforceable against Citrix and others." Dkt. 1 ¶ 28. In fact, prosecution of the '705 patent before the USPTO does not resolve the issue of patent eligibility in this litigation. Indeed, even if the USPTO had considered the applicable *Alice* test during prosecution—which it did not—the claims would nonetheless be squarely subject to review for patent eligibility by the Court. *See PerDiemCo LLC v. NexTraq LLC*, 2024 WL 4521424, at *5 (N.D. Ga. Sept. 26, 2024) ("To the extent PerDiem maintains that this procedural history [that the USPTO granted the patent applications for the Patents-in-Suit] is sufficient to defeat NexTraq's Motion to Dismiss, PerDiem is mistaken. The prosecution history of the Patents-in-Suit or related patents before the USPTO bear no relationship to the subject matter at issue in this Court's Section 101 analysis and in no way shields the patent's

[1] *See Data Health Partners, Inc. v. Teladoc Health, Inc.*, 734 F. Supp. 3d 315, 320 (D. Del. 2024) (courts take judicial notice of prosecution histories for purposes of a motion to dismiss).

claims from Article III review for patent eligibility.") (cleaned up) (citing *Elec. Commc'n Techs., LLC v. ShoppersChoice.com, LLC*, 958 F.3d 1178, 1183 (Fed. Cir. 2020); *TAGI Ventures, LLC v. Turner Sports Interactive, Inc.*, 2017 WL 3469528, at *10 (N.D. Ga. Feb. 17, 2017) (rejecting the same argument)).

### E. Prior Litigation History

K.Mizra contends that "Fortune 100 companies accused of infringing the Asserted Patent have previously filed petitions for IPRs, alleging that the claims of the Asserted Patent should be held invalid as either anticipated or obvious considering art not previously considered." Dkt. 1 ¶ 35.[2] Pursuant to 35 U.S.C. § 311(b), the *inter partes* review ("IPR") process allows the Patent Trial and Appeal Board "to cancel as unpatentable 1 or more claims of a patent ***only on a ground that could be raised under section 102 or 103*** and only on the basis of prior art consisting of patents or printed publications" (emphasis added). As a result, in the IPR proceedings referenced by K.Mizra, the Patent Trial and Appeal Board did not and could not consider patent eligibility based on subject matter under § 101.

## III. LEGAL STANDARDS

Patent eligibility under 35 U.S.C. § 101 is a question of law. *Genetic Techs. Ltd. v. Merial LLC*, 818 F.3d 1369, 1373 (Fed. Cir. 2016); *Implicit LLC v. Home Depot U.S.A., Inc.*, 676 F. Supp. 3d 1312, 1317 (N.D. Ga. 2023). Under 35 U.S.C. § 101, an inventor may obtain a patent for "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." But § 101 "contains an important implicit exception: [l]aws of nature, natural phenomena, and abstract ideas are not patentable." *Alice,* 573 U.S. at 216. Under the Supreme Court's two-step framework for evaluating patent eligibility, a claim falls outside the scope of § 101 if: (1) it is directed to a patent-ineligible concept such as an abstract idea, and (2) it lacks an "inventive concept" sufficient to ensure that the claim amounts to significantly more

[2] K.Mizra alleges that the Federal Circuit "reversed the PTAB's Decision [finding no claims unpatentable] *on a few narrow procedural issues*." Dkt. 1 ¶ 35 (emphasis added). That mischaracterizes the Federal Circuit decision, which stated: "[W]e vacate the Board's motivation to combine analysis, which was rooted in legal error and a fact finding unsupported by substantial evidence. We further vacate the Board's ultimate determination that Cisco failed to show the unpatentability of the challenged claims of the '705 patent and remand for the Board to consider the remaining issues regarding the obviousness of the challenged claims, including Cisco's non-benefits-based motivation to combine arguments and Cisco's fourth rationale." *Cisco Sys., Inc. v. K.Mizra LLC*, 2024 WL 3841809, at *6 (Fed. Cir. Aug. 16, 2024).

than a claim upon the abstract idea itself. *Id.*; *SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1166-67 (Fed. Cir. 2018). "If a patent's recitation of a computer amounts to a mere instruction to implement an abstract idea on a computer, that addition cannot impart patent eligibility." *Alice*, 573 U.S. at 223 (cleaned up).

In evaluating patent eligibility, the Court is "not bound to accept as true a legal conclusion couched as a factual allegation." *Implicit*, 676 F. Supp. 3d at 1318 (quoting *Bell Atl. v. Twombly*, 550 U.S. 544, 555 (2007)) ("The Court is thus not required to accept as true conclusory allegations of eligibility.").[3] "Ultimately, the § 101 inquiry must focus on the language of the [claims] themselves." *ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 769 (Fed. Cir. 2019).

Where the validity of patent claims involves disputed issues of fact, the clear and convincing evidence standard applies for the party challenging validity, but no standard of proof applies where the claims turn "not upon factual disputes, but upon how the law applies to facts as given." *Microsoft Corp. v. I4I Ltd. P'ship*, 564 U.S. 91, 114 (2011) (Breyer, J., concurring); *see Affinity Labs of Tex., LLC v. DirecTV, LLC*, 109 F. Supp. 3d 916, 933 (W.D. Tex. 2015) ("[T]o the extent legal questions bear on the ultimate question of subject matter eligibility, the court will decide those questions as a matter of law . . . ."). "Whether a combination of claim limitations supplies an inventive concept that renders a claim 'significantly more' than an abstract idea to which it is directed is a question of law." *BSG Tech LLC v. Buyseason, Inc.*, 899 F.3d 1281, 1290 (Fed. Cir. 2018). The Federal Circuit has "repeatedly affirmed § 101 rejections at the motion to dismiss stage, before claim construction or significant discovery has commenced." *Elec. Comms. Techs. LLC v. ShoppersChoice.com, LLC*, 958 F.3d 1178, 1184 (Fed. Cir. 2020).

## IV. ARGUMENT

### A. Claim 19 of the '705 Patent is Representative.

"In a § 101 analysis, courts may evaluate representative claims." *Automated Tracking Sols., LLC v. Coca-Cola Co.*, 723 F. App'x 989, 991 (Fed. Cir. 2018) (citing *Content Extraction & Transmission LLC v. Wells Fargo Bank*, 776 F.3d 1343, 1348 (Fed. Cir. 2014)). In determining whether a claim is representative of other claims, courts look to whether claims are "substantially

[3] The *Implicit* court identified that the operative pleading specifically "contain[ed] conclusory allegations of eligibility which the Court need not consider true." Here, Paragraphs 28-34 of K.Mizra's Complaint similarly contain legal conclusions. The Court need not consider those conclusory allegations of eligibility as true.

similar and linked to the same abstract idea." *Content Extraction*, 776 F.3d at 1348 (quoting trial court opinion). Here, K.Mizra reserves the right in its Complaint "to assert additional claims of the Asserted Patent, including both independent and dependent claims." Dkt. 1 ¶ 27. Indeed, K.Mizra refers to these unspecified "additional claims" in its Complaint "as the 'Asserted Claims.'" *Id.*

As other courts have observed, "the Federal Circuit has permitted generic allegations that certain of the defendant's products meet 'each and every element of at least one claim' of the patent-in-suit, [but] a consequence of generic allegations of infringement of one or more claims is that the Court cannot resolve the dispute without determining that [one claim] is representative." *ScanComm LLC v. Block, Inc.*, 2025 WL 1088201, at *5 (N.D. Ga. Mar. 21, 2025) (internal citation omitted) ("ScanComm has left open the possibility that it would seek an infringement judgment based on other claims in the patent."). Here, as in *ScanComm*, claims 1-18 are each substantially similar and linked to the same abstract idea as claim 19, and the other claims have no material differences. *See supra* II.C. Claim 19 of the '705 patent is therefore representative.

### B. The Claims Are Not Patent-Eligible Under 35 U.S.C. § 101.

Under the *Alice* framework, the claims of the '705 patent are directed to a patent-ineligible abstract idea and do not recite an "inventive concept" sufficient to transform them into patent-eligible claims. At step one, the claims are directed to the abstract idea of protecting a network from an infected host through contagion isolation and inoculation. *See* '705 patent, claims 1, 12, and 19 at Preamble ("protecting a network"); Dkt. 1 ¶ 33 ("remediating infected endpoint devices (*e.g.*, host computers) to prevent contagion"); '705 patent, Title ("Contagion Isolation and Inoculation"). The Federal Circuit and district courts have repeatedly held that similar claims, such as those directed to providing restricted access to resources, *Prism*, 696 F. App'x at 1017, controlling access to resources via software, *Ericsson*, 955 F.3d at 1327, and conditioning and controlling access to data, *Smartflash LLC v. Apple Inc.*, 680 F. App'x 977 (Fed. Cir. 2017), constitute patent-ineligible abstract ideas. The same conclusion is required here because the '705 patent improperly claims that very same abstract idea. Indeed, K.Mizra itself alleges that the claims are directed to "detect[ing] an insecure condition by contacting a trusted computing base, receiving a response therefrom, determining whether that response contains a valid identification of cleanliness, and configuring and implementing a remediation action based on what is discovered about the state of an endpoint or 'host' computer." *See* Dkt. 1 ¶ 33.

At step two, the claims recite no inventive concept. The elements recited in the claims, such as a "computer program," "protected network," "host," and "software component" are "indisputably generic computer components." *Prism*, 696 F. App'x at 1017. And the '705 patent itself explains that the recited components intended for a specific use, like the "trusted platform module within the first host," were known, conventional components used for their intended purpose. *Id*. at 1018 ("The patents-in-suit themselves demonstrate the conventional nature of these hardware identifiers… Viewed as an ordered combination, the asserted claims recite no more than the sort of 'perfectly conventional' generic computer components employed in a customary manner that we have previously held insufficient to transform the abstract idea into a patent-eligible invention."). Similar to the claims at issue in *Ericsson*, "[n]one of these elements are sufficient to turn the claim into anything more than a generic computer for performing the abstract idea of controlling access to resources." 955 F.3d at 1330 ("Even assuming that this collection of elements led to a more efficient way of controlling resource access, 'our precedent is clear that merely adding computer functionality to increase the speed or efficiency of the process does not confer patent eligibility on an otherwise abstract idea.'") (quoting *Intell. Ventures I LLC v. Cap. One Bank (USA)*, 792 F.3d 1363, 1370 (Fed. Cir. 2015)).

### 1. *Alice* Step One: The Asserted Claims Are Directed to an Abstract Idea.

The first *Alice* step is the "abstract idea" step, which considers whether the claims are directed to a patent-ineligible concept such as an abstract idea. *Alice*, 573 U.S. at 217; *SAP Am.*, 898 F.3d at 1166-67. Courts ask a variety of questions, addressed below, to determine whether claims are directed to an abstract idea. To answer these questions, courts "focus on the language of the [claims] themselves." *ChargePoint*, 920 F.3d at 769. Here, every inquiry for the *Alice* step one analysis shows the claims are directed to the abstract idea of protecting a network from an infected host through contagion isolation and inoculation.

#### a. Courts Have Held Similar Claims Relating to Controlling Access with Software to Be Directed to an Abstract Idea.

"To determine whether claims are directed to an abstract idea," courts typically "compare the claims at issue to those claims already found to be directed to an abstract idea in previous cases." *Realtime Data LLC v. Array Networks Inc.*, 537 F. Supp. 3d 591, 607 (D. Del. May 4, 2021). The '705 patent claims are directed to protecting a network from an infected host through contagion isolation and inoculation. Courts routinely find similar claims to be directed to abstract ideas.

In *Ericsson*, 955 F.3d at 1325–26, the analysis focused on claims 1 and 5 of the patent at issue in that case, which claimed similar subject matter as the ’705 patent.[4] The Federal Circuit concluded the claims were "directed to the abstract idea of controlling access to, or limiting permission to, resources." *Id.* at 1326. The analysis is instructive here because the Federal Circuit intentionally looked past the "jargon" of a technical patent claim that, by its nature, appeared more complex than it actually was. *Id.* In so doing, the court identified the focus of the claims, and properly set aside the remaining limitations that provided only "necessary antecedent and subsequent components" as inessential for the purpose of the *Alice* step one inquiry. *Id.* The ’705 patent presents similarly, using terms like "trusted computing base" that may be less familiar in ordinary usage, but which refer, as the patent itself explains, merely to a known component used for its conventional purposes of executing antivirus scans or digitally signing software cleanliness assertions. ’705 patent at 14:1-12. When the Federal Circuit evaluated claim 5 in *Ericsson*, a claim that, like the ’705 patent claims, concerns granting access to a network based on particular criteria, the Federal Circuit explained "that the determination to grant access" was directed to an abstract idea. *Id.* at 1327.

Moreover, the Federal Circuit in *Ericsson* set out a helpful roadmap for this Court to follow when considering the similar claims at issue here. The *Ericsson* court explained its analysis as

[4] Claim 1 of patent at issue in *Ericsson*: A system for controlling access to a platform, the system comprising:

a platform having a software services component and an interface component, the interface component having at least one interface for providing access to the software services component for enabling application domain software to be installed, loaded, and run in the platform;

an access controller for controlling access to the software services component by a requesting application domain software via the at least one interface, the access controller comprising:

an interception module for receiving a request from the requesting application domain software to access the software services component;

and a decision entity for determining if the request should be granted wherein the decision entity is a security access manager, the security access manager holding access and permission policies; and

wherein the requesting application domain software is granted access to the software services component via the at least one interface if the request is granted.

Claim 5: The system according to claim 1, wherein:

the security access manager has a record of requesting application domain software; and the security access manager determines if the request should be granted based on an identification stored in the record.

follows:

> ***[W]e have repeatedly found the concept of controlling access to resources via software to be an abstract idea***. *See Smart Sys. Innovations, LLC v. Chicago Transit Authority*, 873 F.3d 1364, 1371 (Fed. Cir. 2017) (claim involving "denying access to a transit system if the bankcard is invalid" was directed to an abstract idea); [*Prism*, 696 F. App'x at 1017] (***abstract idea of "providing restricted access to resources"***); [*Smartflash*, 680 F. App'x at 982] (***abstract idea of "conditioning and controlling access to data"***). The claims at issue here are no different.

*Id.* (emphases added). The cases cited in *Ericsson* each involve patent claims directed to systems and methods that, like the '705 patent, describe computer networking solutions for access control with secure processes that automatically identify, restrict, or permit access based on designated criteria. In each case, the Federal Circuit concluded these claims are directed to abstract ideas.

District courts in this Circuit have reached similar conclusions. For example, in *Digital Media Technologies*, 2017 WL 4750705, the court examined a claim related to protecting the content distributed on a network. *Id.* at *2. The patent at issue there described a solution remarkably similar to the solution proposed in the claims of the '705 patent: performing authentication checks for authorization, validating authentication information based on predetermined criteria, and taking steps to either allow or not allow access to the secured resource, using a specialized content server to control and perform aspects of the authentication process.[5]

[5] Claim at issue in *Digital Media Technologies*:
A multimedia system, comprising:

an external control server configured to:

receive a request from a client device via a wide area network requesting protected content to be sent to the client device;

receive client device authentication information from the client device, the client device authentication information comprising at least information related to a user authentication and a device authorization;

validate the client device authentication information according to predetermined criteria;

send protected content location information to the client device, the protected content location information being associated with a location of the protected content;

encrypt, in response to receiving a request for a content license from the client device via the wide area network, the request comprising information related to a location of the content license and being based on a determination by the client device that the protected content is encrypted and requires a content license, the content license using a public key associated with the client device, the content license comprising a content key which the client device uses to decrypt the protected content and usage parameters specifying the terms under which the protected content can be consumed; and

send the encrypted content license to the client device, the client device using a private key associated with the client device to decrypt the content license and using the content key to decrypt

The party challenging the validity of the patent contended it was ineligible for protection under § 101 because it claimed "the abstract and ancient idea of limiting access to content to authorized users." *Id.* at *3. The court held the claim should be considered as directed either to the abstract idea of "secured content-delivery," or, alternatively, "the abstract idea of delivering content secured with licenses and encryption." *Id.* at *5.

Similarly, in *Prism,* 696 F. App'x at 1016, the Federal Circuit explained that a claim directed to the abstract idea of "providing restricted access to resources" is patent-ineligible.[6] There, the Federal Circuit analyzed the claim and found it "directed to an abstract process that includes: (1) receiving identity data from a device with a request for access to resources; (2) confirming the authenticity of the identity data associated with that device; (3) determining whether the device identified is authorized to access the resources requested; and (4) if authorized, permitting access to the requested resources." *Id.* at 1017. These steps are strikingly similar to the four steps K.Mizra described as the focus of the claims of the '705 patent. *See* Dkt. 1 ¶ 34.

In sum, a wealth of precedential case law from the Federal Circuit and from district courts in this Circuit confirms that the claims of the '705 patent are directed to the abstract idea of

the protected content for use according to usage parameters specified by the content license;
and
an external content server configured to:
receive a request for the protected content from the client device, the request comprising the protected content location information provided by the external control server; and
send the protected content to the client device.

[6] Claim at issue in *Prism*:
A method for controlling access, by at least one authentication server, to protected computer resources provided via an Internet Protocol network, the method comprising:
receiving, at the at least one authentication server from at least one access server, identity data associated with at least one client computer device, the identity data forwarded to the at least one access server from the at least one client computer device with a request from the at least one client computer device for the protected computer resources;
authenticating, by the at least one authentication server, the identity data received from the at least one access server, the identity data being stored in the at least one authentication server;
authorizing, by the at least one authentication server, the at least one client computer device to receive at least a portion of the protected computer resources requested by the at least one client computer device, based on data associated with the requested protected computer resources stored in at least one database associated with the at least one authentication server; and
permitting access, by the at least one authentication server, to the at least the portion of the protected computer resources upon successfully authenticating the identity data and upon successfully authorizing the at least one client computer device.

protecting a network from an infected host through contagion isolation and inoculation. In *Prism*, for example, the Federal Circuit held that providing restricted access to resources is an abstract idea. In *Ericsson*, the Federal Circuit confirmed that controlling access to, or limiting permission to, resources is also an abstract idea. The asserted claims here are no different, requiring the protection of a network from an infected host through contagion isolation and inoculation.

#### b. The Claims Recite Generalized Steps Performed Using Conventional Computer Activity and Components.

The next question asked as part of the *Alice* step one analysis is whether the claims recite "[g]eneralized steps to be performed on a computer using conventional computer activity." *Dropbox, Inc. v. Synchronoss Techs., Inc.*, 815 F. App'x 529, 537 (Fed. Cir. 2020) (quoting *RecogniCorp, LLC v. Nintendo Co.*, 855 F.3d 1322, 1326 (Fed. Cir. 2017)). Many elements recited in the claims of the '705 patent are plainly generic, such as a "computer program," "protected network," "host," and "software component." Moreover, these components are used only to perform conventional activities in the context of the claims.

The claims of the '705 patent do recite technology terms that are less commonly used, but the patent specification confirms these terms refer to known components used for their conventional purpose. The patent confirms, for example, it did not invent "contacting a trusted computing base within a computer"; rather, the '705 patent discloses examples that had already been invented. '705 patent at 14:1-7. The '705 patent also explains its reference to contacting a trusted computing base is for a conventional purpose, "for example execut[ing] antivirus scans of the remainder of the computer" or "digitally sign[ing] assertions about the cleanliness (e.g. infestation status) and/or state of their computers." *Id.* at 14:7-12.

The claims of the '705 patent are directed to protecting a network from an infected host through contagion isolation and inoculation. Because the steps of the claims are performed only using known, conventional computer components to perform the conventional activity of access control, the claims are directed to an abstract idea. Furthermore, implementing the abstract ideas of resource protection and access control in a network environment changes nothing, because an "abstract idea does not become nonabstract by limiting the invention to a particular field of use or technological environment, such as the Internet." *See Alice,* 573 U.S. at 222 (limiting an abstract idea to a particular technological environment, such as a computer, does not confer patent eligibility); *Bilski v. Kappos,* 561 U.S. 593, 612 (2010) ("[L]imiting an abstract idea to one field of use . . . d[oes] not make the concept patentable.").

#### c. The Claims of ’705 Patent Are Directed to an Idea that Is Pervasive in Human Activity.

The Supreme Court has explained that the category of abstract ideas embraces “fundamental economic practice[s] long prevalent in our system of commerce,” including “longstanding commercial practice[s]” and “method[s] of organizing human activity.” *Alice*, 573 U.S. at 220; *see also MModal Servs. Ltd. v. Nuance Commc’ns, Inc.*, 2019 WL 13059774, at *3 (N.D. Ga. May 13, 2019). The claims of the ’705 patent recite a process for safeguarding computer networks, but that process simply mirrors a method of organizing human activity to mitigate contagion through isolation (*i.e.*, quarantine) and inoculation (*i.e.*, remediation).

The Federal Circuit in *Ericsson* made precisely this point. It explained:

> Controlling access to resources is exactly the sort of process that ‘can be performed in the human mind, or by a human using a pen and paper,’ which we have repeatedly found unpatentable. *See CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1372 (Fed. Cir. 2011). The idea long predates the ’510 patent and is pervasive in human activity, whether in libraries (loaning materials only to card-holding members), office buildings (allowing certain employees entrance to only certain floors), or banks (offering or denying loans to applicants based on suitability and intended use). In each of these circumstances, as in the claims at issue, a request is made for access to a resource, that request is received and evaluated, and then the request is either granted or not.

*Ericsson*, 955 F.3d at 1327. K.Mizra emphatically protests that the claims of the ’705 patent are not directed “simply [to] quarantining an infected device.” Dkt. 1 ¶ 33. But every single element of the claims, including directing a host toward sources for obtaining inoculation and automation of the isolation process, is mirrored by the age-old process of restricting access to potentially infected hosts through quarantine. *See supra* II.B. The patent therefore improperly claims an abstract idea in the form of a method of organizing human activity and merely applies that abstract idea to a particular technological environment. As the Supreme Court has explained, limiting an abstract idea to a particular technological environment, such as a computer, does not confer patent eligibility. *Alice,* 573 U.S. at 222. The claims of the ’705 patent are accordingly directed to an abstract idea.

### 2. *Alice* Step Two: The Asserted Claims Recite No Inventive Concept.

Because the asserted claims are directed to an abstract idea, this Court must next consider, at step two of the *Alice* framework, whether the claims contain an inventive concept that amounts to significantly more than just the abstract idea itself. *Alice*, 573 U.S. at 217-18. Any such "inventive concept" must be more than a "well-understood, routine, conventional" activity. *Id.* at 225. With regard to the '705 patent, there is not "anything inventive in the ordered combination of the claim limitations" where this combination constitutes "merely reciting an abstract idea performed on a set of generic computer components." *Hawk Tech. Systems, LLC v. Castle Retail, LLC*, 60 F.4th 1349, 1359 (Fed. Cir. 2023). K.Mizra erroneously relies on the *specification* of the '705 patent when it alleges that the *claims* contain inventive concepts, but in the context of the § 101 inquiry, "detail from the specification" cannot be used to argue that claims are directed to inventive concepts, "if those details are not claimed." *ChargePoint*, 920 F.3d at 769. Rather, "any reliance on the specification in the § 101 analysis must always yield to the claim language." *Id.* Finally, the ordered combination of steps in the claims cannot supply an inventive concept because this combination of steps was already well known at the time of the priority date of the '705 patent, as K.Mizra acknowledges.

First, the "the asserted claims recite no more than the sort of 'perfectly conventional' generic computer components employed in a customary manner." *Prism*, 696 F. App'x at 1018 (citing *Intell. Ventures*, 838 F.3d at 1321). As explained above, the elements recited in the claims, such as a "computer program," "protected network," "host," and "software component" are "generic computer components." *Id.* at 1017. Just like in the *Prism* case, "[t]he patents-in-suit themselves demonstrate the conventional nature of these hardware identifiers." *Id.* at 1018. The '705 patent describes how components intended for a specific use, like the "trusted platform module within the first host," were known, conventional components being used for their intended purpose. Indeed, even the function of the claims reflects a conventional usage of known components. For example, elements E, E1, and E2 of claim 19 recite:

> [E] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes
>
> > [E1] receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request,
> >
> > [E2] and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition;

But this decision tree of choices (*see* '705 patent, Fig. 16) simply amounts to conventional ways of re-routing internet traffic away from the protected network to a quarantine server. By analogy, if a sick child arrived at the entrance of a school and asked to be let inside (i.e., the "web server request"), the doors would be shut, and the child would be told to go to an immunization clinic (i.e., the "quarantine notification page"). If a sick child called the school and asked for the school's address (i.e., the "DNS (domain name server) query"), the child would instead be told the address for an immunization clinic's location (i.e., the "IP address of a quarantine server"). The steps of the claims amount to nothing more than "well-understood, routine, conventional activity." *Alice*, 573 U.S. at 225 (cleaned up). And the Federal Circuit has repeatedly held that the claims' recitation of "generic computer components employed in a customary manner" is "insufficient to transform the abstract idea into a patent-eligible invention." *Prism*, 696 F. App'x at 1018.

Second, K.Mizra's allegations regarding the validity of the '705 patent's claims should be set aside as conclusory. As noted above, the Court is not required to accept as true any of K.Mizra's legal conclusions masquerading as factual allegations. For example, K.Mizra's conclusory claim that, "[n]one of the Asserted Claims are directed to abstract ideas, and each employs inventive concepts and is directed to patent-eligible subject matter," is neither a factual statement, nor is it correct. Dkt. 1 ¶ 28.

Additionally, because K.Mizra's allegations regarding patent eligibility rely upon the patent specification, not the claims, the allegations should also be set aside as irrelevant. *See* Dkt. 1 ¶¶ 29-31, 33. The Federal Circuit has explained that a patent plaintiff cannot save its claims at step two of the *Alice* inquiry by pointing to details from the specification. *See ChargePoint*, 920 F.3d at 769 ("Even a specification full of technical details about a physical invention may nonetheless conclude with claims that claim nothing more than the broad law or abstract idea underlying the claims.").

After setting aside K.Mizra's legal conclusions and citations to the patent specification, the remaining allegations are insufficient because they merely reference technical jargon intended to make the claims' conventional use of known computer components appear more complex. *See, e.g., id.* ¶ 32 (alleging that quarantining hosts "requires the involvement of various hardware components running dedicated software" to "automatically and dynamically" isolate an unsafe device). Even accepted as true, these allegations are insufficient because the "various hardware components" were known, and the "dedicated software" performs conventional functions. *See supra* IV.B.1.b.

Moreover, even if it were true that the claims could be characterized as "removing the once-necessary human intervention from a fundamentally mechanical process," resulting in "an improvement in the functioning of a networked system," that still would not be enough. Dkt. 1 ¶ 32. To the contrary, "[e]ven assuming that this collection of elements led to a more efficient way of controlling resource access, '[Federal Circuit] precedent is clear that merely adding computer functionality to increase the speed or efficiency of the process does not confer patent eligibility on an otherwise abstract idea.'" *Ericsson*, 955 F.3d at 1330 (Fed. Cir. 2020) (quoting *Intell. Ventures*, 792 F.3d at 1370). Indeed, K.Mizra's own characterization of the claims of the '705 patent shows they are directed to an abstract idea implemented on a computer. Dkt. 1 ¶ 34.

The Court is not required to accept K.Mizra's legal conclusions as true, but accepting its assertions changes little. K.Mizra claims "the improvement captured by the Asserted Claims is not simply quarantining an infected device, but it is instead a multi-faceted network system involving multiple interrelated software and hardware components to protect a network from known and unknown threats." Dkt. 1 ¶ 33. Protecting a network "from known and unknown threats" using "multiple" components is nothing more than the abstract idea of protecting a network from an infected host through contagion isolation and inoculation. Indeed, the essential premise of quarantine is a blanket exclusion of unverified entities due to potential exposure to the unknown. And the "multi-faceted network system" in K.Mizra's allegation is the internet, so K.Mizra's jargon-laden circumlocution amounts to quarantining a computer from threats on the internet. For purposes of the *Alice* step two analysis, a "simple instruction to apply an abstract idea on a computer is not enough." *Intell. Ventures*, 792 F.3d at 1367 (citing *Alice,* 573 U.S. at 523); *Alice,* 573 U.S. at 523 ("[R]ecitation of a generic computer cannot transform a patent-ineligible idea into a patent-eligible invention. Stating an abstract idea 'while adding the words "apply it" is not enough for patent eligibility.'").

Third, as *Digital Media Technologies* compellingly explains, the individual steps of the '705 patent claims can only be considered well-understood, routine, and conventional. In particular, "it is nothing new for servers and clients to send requests to each other," "it is not inventive to require authentications to access content," and the "use of an 'access mechanism' to enforce . . . pre-selected rules is nothing more than programming conventional software or hardware to apply rules governing access—a routine, conventional practice." 2017 WL 4750705, at *5 (citing *Fitbit, Inc v. AliphCom*, 2017 WL 528491, at *8 (N.D. Cal. Feb. 9, 2017) (holding that generic recitations of communications between servers and clients did not provide inventive concept); *OpenTV, Inc. v. Apple Inc.*, 2016 WL 344845, at *5 (N.D. Cal. Jan. 28, 2016) ("The practice of controlling access to information by verifying credentials ... is a long-standing and well-understood business practice that predates the internet."); *Uniloc USA, Inc. v. Amazon.com, Inc.*, 2017 WL 1049595 (E.D. Tex. Mar. 20, 2017); *Intell. Ventures II LLC v. JP Morgan Chase & Co.*, 2015 WL 1941331, at *14 (S.D.N.Y. Apr. 28, 2015) ("The use of an 'access mechanism' to enforce ... pre-selected rules is nothing more than programming conventional software or hardware to apply rules governing access—a routine, conventional practice.").

In light of these collected cases and their clear application to the claims of the '705 patent, "the only real issue is whether the ordered combination of claim elements supplies an inventive concept." *Digital Media Techs.*, 2017 WL 4750705, at *6. Here, the ordered combination of claim elements do not supply any inventive concept because the '705 patent itself describes how components intended for a specific use, like the "trusted platform module within the first host," were known, conventional components being used for their intended purpose. Moreover, the state of the art at the priority date of the '705 patent already encompassed the ordered combination of its steps, which were widely recognized in ordinary human activities like school enrollment. The claims of the '705 patent therefore cannot overcome the *Alice* step two inquiry because they recite no inventive concept sufficient to transform the abstract idea into patentable subject matter.

### C. This Issue is Appropriate for Resolution.

Granting a motion to dismiss with prejudice pursuant to Federal Rule of Civil Procedure 12(b)(6) is the appropriate remedy when a plaintiff asserts patent claims that "are drawn to ineligible subject matter under 35 U.S.C. § 101." *BSG Tech LLC v. AutoZone, Inc.*, 2017 WL 2609066, at *5–6 (E.D. Tex. Mar. 30, 2017). Courts regularly grant dismissal with prejudice in patent cases at this stage of proceedings. *See id.*; *see also Validity, Inc. v. Project Bordeaux, Inc.*, 2023 WL 6200287, at *12 (D. Del. Sept. 22, 2023). Indeed, the Federal Circuit has "repeatedly affirmed § 101 rejections at the motion to dismiss stage, before claim construction or significant discovery has commenced." *Elec. Comms. Techs. LLC*, 958 F.3d at 1184 (quoting *Cleveland Clinic Found. v. True Health Diagnostics LLC*, 859 F.3d 1352, 1360 (Fed. Cir. 2017)).

## V. CONCLUSION

For the foregoing reasons, Defendants respectfully requests that the Court grant its motion and dismiss with prejudice K.Mizra's Complaint alleging that Defendants infringe the '705 patent.

Dated: June 10, 2025

Respectfully submitted,

**DLA PIPER LLP (US)**

*/s/ Ardith Bronson*
Ardith Bronson, Esq.
Florida Bar Number: 423025
ardith.bronson@us.dlapiper.com
DLA Piper LLP (US)
200 South Biscayne Boulevard
Suite 2500
Miami, Florida 33131
Telephone: (305) 423-8562

*Counsel for Defendants Citrix System, Inc.*
*and Cloud Software Group, Inc.*

## CERTIFICATE OF SERVICE

I hereby certify that on June 10, 2025, I electronically filed the foregoing document via CM/ECF, which caused a true and correct copy to be served electronically upon all entitled parties.

*/s/ Ardith Bronson*
Ardith Bronson, Esq.